REMARKS

A. GENERALLY

Claims 1-14 and 18-26 remain in this application. Claims 13 and 18-26 have been withdrawn. Claims 15-17 and 27-32 were previously canceled. Thus, claims 1-13 were examined. Claim 1 has been amended. No new matter has been added.

B. CLAIM REJECTIONS

1. Claims 1, 2, 4, 5 and 13 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Pat. No. 5,586,260 issued to Hu (hereinafter, "Hu").

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). (MPEP §2131, 8th Ed. (Rev. 1).)

Hu describes a method and corresponding apparatus for authenticating a client for a server when the client and server have different security mechanisms. An authentication gateway authenticates a client using the client security mechanism and impersonates the client in a call to a server that the client wishes to access. Thus, the communications between the client and the server are passed through the authentication gateway. "When the client wishes to call the server, the client calls the authentication gateway acting as a proxy server, and passes the access key, which is then used to retrieve the security credentials and to impersonate the client in a call to the server. Any output arguments resulting from the call to the server are returned to the client through the authentication gateway." (See, Hu, Abstract).

Hu describes a proxy server (residing on the authentication gateway) that brokers communications between a user and a server when the user does not conform to the security protocol of the server. According to Hu, a client does not need to be registered with a proxy server that it might use. (See, Hu, Col. 7, lines 11-16). Thus, Hu does not teach or reasonably suggest registering users with a discovery machine and establishing a direct link between the client and the server as recited in independent claim 1 (as amended) of the present application.

To make this clear, Table 1 below provides a mapping of the limitations of claim 1 (as amended) to the cited disclosures of Hu. The claim limitations have been labeled for ease of discussion.

TABLE 1

CLAIM 1 LIMITATIONS	REFERENCES CITED IN OFFICE ACTION
1. A method for communication over a network that allows for the authentication of individuals and control of information comprising:	
(a) registering with a discovery machine a first user and a second user, wherein said first user maintains a first client machine and said second user maintains a second client machine, wherein said first client machine, said second client machine and said discovery machine are coupled to a network;	FIG. 3 takes the explanation of the authentication gateway scheme one step further, and shows diagrammatically the sequence of steps followed by each of the systems in handling access to the server 12 by a client system 10 not conforming with the security mechanism of the server. The client system 10 includes a log-in procedure 30, and a client application process 32 from which a server request will emanate. The log-in procedure 30 is executed, as its name implies, only infrequently, such as once a day. Part of the log-in procedure is a call to the authentication gateway 22 to permit authentication within the client security domain. This call, indicated by line 34 carries as parameters the identity of the client and any necessary password or security code needed to satisfy the security requirements of the client security domain. The authentication gateway 22 performs the operations necessary to verify the authenticity of the client 10. The authentication gateway 22 acquires authentication credentials for the client and saves them for later use. The authentication gateway 22 then returns to the log-in procedure 30, over line 36, an identifier that confirms authentication of the client. The log-in procedure 30 stores the returned identifier in an id. cache 38. This completes the first phase of operation of the gateway, which has authenticated the client within the client's security domain and has stored a confirming identifier in the cache 38, over line 40 for later use by the client. Hu, Col. 4, lines 17-43.
(b) initiating a communication from said second user via said second client machine to said first user via said first client machine through said	When the client application process 32 later makes a request to a server, the client process first retrieves the server-domain identity from the id. cache 38, and passes this information to the proxy server. The specific mechanism for passing this information to the proxy server depends on the application, but could, for example, pass the identity as an argument of another

discovery machine;	remote procedure call (RPC) used to invoke the server request. The proxy server receives the RPC from the client and obtains the client's authenticated identity by calling the authentication gateway, using the server-based identifier passed from the client application. The proxy server then impersonates the client and makes another RPC call to the real server. The server returns any output arguments to the proxy server, and the latter returns the output arguments to the client application. The proxy server may then resume its own identity. Hu, Col. 5, lines 41-58.
(c) the discovery machine determining that said first user will accept said communication;	The proxy server process 20 then uses the server-based id. to retrieve the client security context to impersonate the client, and makes a call to the server 12 using the appropriate server credentials, as indicated in block 62. Hu, Col. 6, lines 30-33.
(d) the discovery machine establishing a direct link between said first client machine and said second client machine; and delivering said communication over said direct link;	Figure 4
(e) wherein said direct link is not established if said first user does not accept said communication.	"access to the server requires authentication of client."

As to limitations 1(a) and 1(b), the cited text describes authenticating a client with an authentication gateway. However, the authentication gateway does not perform the functions of establishing a communication between a first client machine and a second client machine as recited in limitation 1(b). Rather, Hu teaches that communications are performed by a proxy server (see text cited in reference to limitation 1(b). Hu acknowledges that users are not registered with the proxy server (the device that Hu describes as establishing communications between a client and a server):

> Because the procedure requires no modification of the server, it works with multiple servers. Moreover the procedure can be easily modified to work with different client security domains. The method of the invention is virtually "transparent" to client application processes, which do not need to change their calling interfaces. Further, the proxy server has no significant management overhead. The proxy server does not store a client's secret key (server-based id.), and does not need to manage user accounts. For example, a client does not need to be registered with a proxy server that it might use.

> Management overhead is further reduced because the proxy server has precisely the same privileges as the client on whose behalf it is acting. (Hu, Col. 7, lines 7-18; emphasis added by underlining.)

Additionally, the cited text does not describe registering a second user (the server 12, for example) with the authentication gateway or the proxy server.

As to limitation (d) (as amended), "the discovery machine establishing a direct link between said first client machine and said second client machine; and delivering said communication over said direct link," and limitation (e), "wherein said direct link is not established if said first user does not accept said communication," Hu does not teach or reasonably suggest that a direct link is established between a first client machine and a second client machine. Rather, Hu repeatedly describes the use of a proxy server between a client and a server:

> Subsequently, when the client application process 32 wishes to make a call to the server, the contents of the id. cache are retrieved, as indicated by the broken line 42, and the client makes a call to the proxy server process 20, as indicated by line 42, passing as an argument of the call the identifier obtained from the cache 38. Then, using the identifier, the proxy server 20 calls the authentication gateway 22, as indicated by line 44, and acquires, over line 46, the credentials of the client that were saved by the authentication gateway during the log-in procedure. At this point the proxy server has all the information it needs to make a call to the real server 12, as indicated by line 48. Information generated as a result of the call to the server 12 is passed back to the client application process 32, through lines 48 and 43. (Hu, Col. 4, lines 44-58; emphasis added by underlining.)

Figure 4 of Hu, cited in the office action as teaching limitation (d), further confirms that communications pass through the proxy server 20. In describing the operations illustrated in Figure 4, Hu states:

> The proxy server process 20 then uses the server-based id. to retrieve the client security context to impersonate the client, and makes a call to the server 12 using the appropriate server credentials, as indicated in block 62. The server 12 processes the call and returns any required output arguments, as indicated by line 64. The output arguments are passed, in turn, back to the client application process, as indicated by block 66 in the proxy server process 20, and block 68 in the client system 10. (Hu, Col. 6, lines 30-38; emphasis added by underlining.)

Hu further derides allowing clients to communicate with each other directly:

> A possible alternative solution to this problem uses a mechanism known as delegation. The client delegates its authority to a proxy server to act as the client in certain respects.

> However, some security mechanisms do not support the delegation mechanism. Another alternative is to modify the server to support both forms of security mechanism, but this is inconvenient since it may require modification of a number of different servers of interest. Yet another approach is to embed passwords in the client application code, to be used to log onto the server system directly. The main objection to this is that it is not a good practice from a security standpoint. Another solution is to have the client send a password every time a server application is invoked, but this is cumbersome for the user and also poses security risks. (Hu, Col. 3, lines 30-45; emphasis added by underlining.)

Based on the foregoing, Applicant submits that Hu does not teach or reasonably suggest all of the limitations of claim 1 (as amended). Claim 1 (as amended) is not, therefore, anticipated by Hu. Claims 2-13 depend from claim 1 (as amended) and are thus not anticipated by Hu.

2. Claims 1, 2, 4, 6-11 and 13 have been rejected under 35 U.S.C. § 103(c) as being obvious over Mathis et al. (U.S. Pat. No. 5,054,019) in view of Edelstein et al. (U.S. Pat. No. 5,764,906).

To establish a prima facie case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. (MPEP §2142, 8th Ed.)

To make this clear, Table 2 below provides a mapping of the limitations of claim 1 to the cited disclosures of Mathis and Edelstein. The claim limitations have been labeled for ease of discussion.

TABLE 2

CLAIM 1 LIMITATIONS	REFERENCES CITED IN OFFICE ACTION
1. (Original) A method for communication over a network that allows for the authentication of individuals and control of information comprising:	
(a) registering with a discovery machine a first user and a second user, wherein said first user maintains a first client machine and said second user maintains a second client machine, wherein said first client	This invention deals with a mnemonic denotation system for Electronic Resources on a Network such as the Internet and a concomitant system of request and delivery services for these Electronic Resources. Specifically, this invention is a system for providing and maintaining short aliases for information resources and their providers and a system for translation of these aliases to meaningful electronic addresses such as URL's, facsimile and voice telephone numbers and electronic mail

machine, said second client machine and said discovery machine are coupled to a network;	addresses, and for accessing the resources by means of these addresses. The system according to the invention need not implement an information utility, nor need it store the information which information providers make available to user communities. Nor does a system according to the invention need to classify or index information in such a utility or network. This invention concerns itself primarily with a system for "aliasing" information resources with short mnemonic names chosen by the information providers and with a system for providing users with pointers to (access to) the information or actually delivering the information in a variety of formats on behalf of the information providers. Edelstein, Col. 3, lines 40-60; Fig. 5. Clients are used by information providers in order to make their resources accessible to users by registering Source and Resource Aliases and providing information associated with those Aliases. The Client sites retain a collection of recently used Resource Aliases and their related data including, but not limited to, the Addresses of the Electronic Resources associated with the Resource Aliases and descriptions of those Resources. The site is able to present the Resource Alias-related data to users, accept requests for retrieval of Resource Alias-related data, and invoke other software which may be resident on the same or other computers (such as World Wide Web browsers) in order to actually retrieve the Resources which the Resource Aliases represent. Client site requests for Resource Alias-related data are relayed to Local Servers which may either have such data cached (locally stored) or which may in turn request that information from the Central Registry or a Root Server on behalf of the Clients. The Client site may also accept requests for registration of new Resource or Source aliases on behalf of their users (who happen to be information providers) and submit those requests to the Central Registry (possibly via a Local Server). An important feature of the Client site is the ability to accept user requests for the "delivery" of the Electronic Resource associated with a Resource Alias. The satisfaction of this type of request may, take on several forms, including but not limited to: (1) invoking a software program such as a web browser, Gopher program or FTP (file transfer program) to access the document or resource, (2) sending a request to a Value Added Server to transmit the Resource in question to the user by postal service, electronic mail or facsimile, and (3) sending a request to a special server which provides direct voice telephone

	transmission of the information in the Resource to the user (either by human voice or by synthetic electronic voice). Edelstein, Col. 6, lines 32-66.
(b) initiating a communication from said second user via said second client machine to said first user via said first client machine through said discovery machine;	Id.
(c) the discovery machine determining that said first user will accept said communication;	T determines whether it will accept a link request 28. Mathias, Col. 3 lines 39-40. The target node decides whether it will accept the atomic action request 38. Mathias, Col. 3, lines 54-55
(d) the discovery machine establishing a direct link between said first client machine and said second client machine; and delivering said communication over said direct link;	If the target node will accept the request, it transmits a turnaround message 44 to the initiating node. The turnaround message provides several functions. It acts as an acknowledgement to the last data block transmitted by the initiating node. It also indicates that the request was granted, implying that data transmission will now change direction, and acts as a request to transmit data to the initiating node. In response to the turnaround message, the initiating node I transmits its receiving parameters 46 to the target node T. As described above, these parameters preferably include the number of available buffers in node I, and the buffer size. The target node T then sends data 48 to the initiating node I. The final block of data contains a flag which indicates that it is the final data block of this transfer. When the initiating node I acknowledges the final block of data, it disconnects the communication link 50 and the atomic operation is complete. Mathias, Col. 3, line 63 through Col. 4, line 12.
(e) wherein said direct link is not established if said first user does not accept said communication.	If not, T denies the request 30 and disconnects the link 32. Mathias, Col. 3, lines 40-41.

The office action asserts that that Mathis teaches limitations 1(c)-1(e) of claim 1 as examined. The office action concedes that Mathis does not disclose limitation 1(a), "registering with a discovery machine a first user and a second user" and limitation 1(b), "initiating a communication from said second user via said second client machine to said first user via said first client machine through said discovery machine." These limitations are said to be found in Edelstein.

As to limitation 1(a), the Edelstein reference describes a client computer having access to aliasing information but does not teaches registering a user for access to various network resources. Rather, the registration described in Edelstein is directed to the registration of source aliases. Thus, Edelstein does not teach that multiple users are registered for access to one another after both have registered. Thus, Edelstein not teach or reasonably suggest limitation 1(a).

The office action acknowledges that Mathis does not teach or reasonably suggest limitation 1(b), "initiating a communication from said second user via said second client machine to said first user via said first client machine through said discovery machine." The office action asserts that the central registry disclosed by Edelstein performs the functions recited in limitation 1(b). However, the central registry described by Edelstein does not broker communications between two registered users as described in limitation 1(b). Edelstein does not expressly describe the registration of users (only the registration of alias information) and cannot perform the functions described in this limitation.

As to limitation 1(c), "at the discovery machine, determining that said first user will accept said communication," the office action asserts that Mathis teaches this limitation. However, the language of Mathis cited by the office action as reading on this limitation makes it clear that the determination of whether the first user will accept a communication is made by the target node, not a discovery machine:

> T determines whether it will accept a link request 28. (Mathias, Col. 3 lines 39-40.)
>
> And:
>
> The target node decides whether it will accept the atomic action request 38. (Mathias, Col. 3, lines 54-55.)

Mathis does not, therefore, teach or reasonably suggest limitation 1(c).

As to limitation 1(e), the text cited by the office action makes it clear that the determination not to establish a link between the initiating node and the target node is made by the target node, not the discovery machine. Mathis does not, therefore, teach or reasonably suggest limitation 1(e).

Because the combination of Mathis and Edelstein fails to teach or reasonably suggest all of the limitations of claim 1 (as amended), claim 1 (as amended) is patentable over that combination. Additionally, because claims 2, 4, 6-11 and 13 depend from claim 1 (as amended), claims 2, 4, 6-11 and 13 are patentable over the cited combination.

3. Claim 12 has been rejected under 35 U.S.C. § 103(c) as being obvious over Mathis in view of Edelstein and further in view of U.S. Pat. No. 6,185,611 issued to Waldo et al. (hereinafter, "Waldo").

Claim 12, which depends from claim 1 (as amended), recites the limitation, "wherein determining that said first user will accept said communication further comprises the step of storing notification of said communication if said first user is unavailable." The office asserts that this limitation may be found in Waldo.

Applicant submits that there is no motivation to combine Waldo with Mathis and Edelstein. Mathis is cited as teaching the determining that a user will accept a communication. As noted above, Mathis teaches that this determination is made by the target node. The office action asserts that it "one would have obvious to one of ordinary skill in the art at the time the invention was made for the step of determining that the first user will accept the communication to further comprise the step of storing the notification of the communication if the first user is unavailable. One would be motivated to do so for clients to avoid attempting to access a service that is no longer available (Waldo, Abstract)." (Office Action, p. 8.)

Applicant respectfully submits that the suggested motivation fails to identify a structure that would perform this step. Mathis does not teach a discovery machine. Thus, the only candidate for performing the suggested step is the initiating node. However, in order to store information regarding a failed communication at the initiating node, the initiating node would have to support additional structures capable of knowing the state of the target nodes in the network and capable of updating this state information as the state of the target nodes change. Such a modification of Mathis would impermissibly change the theory of operation of Mathis. Based on the foregoing, Applicant submits that there is no motivation to combine Mathis and Edelstein with Waldo.

Additionally, Applicant has previously demonstrated that the combination of Mathis and Edelstein fails to teach the limitations of claim 1 (as amended). Because claim 12 depends from claim 1 (as amended), claim 12 recites the limitations of that base claim. Waldo is not cited by the office action as curing the deficiencies of the combination of Mathis and Edelstein. For these reasons, claim 12 is patentable over the combination of Mathis, Edelstein and Waldo.

4. Claims 1-4, 6-8 and 13 have been rejected under 35 U.S.C. § 103(c) as being obvious over Mathis in view of U.S. Pat. No. 6,941,148 issued to Hansmann et al. (hereinafter, "Hansmann").

Referring to the labeled limitations of claim 1 (as amended) listed in **Table 2** above, the office action asserts that that Mathias teaches limitations 1(c)-1(e) of claim 1 as examined. The office action concedes that Mathis does not disclose limitation 1(a), "registering with a discovery machine a first user and a second user" and limitation 1(b), "initiating a communication from said second user via said second client machine to said first user via said first client machine through said discovery machine." These limitations are said to be found in Hansmann.

Applicant further submits that there is no motivation to combine Mathis and Hansmann. Mathis describes a process by which nodes in a network establish a two-way communication. Hansmann describes a process for using icons to permit a wireless device to communicate with a backend system. The office action asserts that one would be motivated to combine Mathis and Hansmann to provide "a more flexible means of connecting a client to a plurality of other nodes as taught by Hansmann." (Office Action, p. 11.) Applicant respectfully submits that the suggested motivation fails to identify a structure that would perform this step. Mathis does not teach a discovery machine or a central server. Adding a central server to Mathis amounts to impermissible hide sight in which the blueprint for the combination is the disclosure of the present application. Based on the foregoing, Applicant submits that there is no motivation to combine Mathis and Hansmann.

Even assuming that Mathis and Hansmann may be combined, the combination does not expressly teach registering a user with a discovery machine. Hansmann does not teach registering two users so as to facilitate communications between them. Hansmann does not, therefore, teach limitation 1(a).

The office action acknowledges that Mathis does not teach or reasonably suggest limitation 1(b), "initiating a communication from said second user via said second client machine to said first user via said first client machine through said discovery machine." The office action asserts that this limitation is met by a central registry that connects a user with a backend system. However, the central registry described by Hansmann does not broker communications between two registered users as described in limitation 1(b).

As to limitation 1(c), "at the discovery machine, determining that said first user will accept said communication," the office action asserts that Mathis teaches this limitation. However, the language of Mathis cited by the office action as reading on this limitation makes it clear that the determination of whether the first user will accept a communication is made by the target node, not a discovery machine:

> T determines whether it will accept a link request 28. (Mathias, Col. 3 lines 39-40.)
>
> And:
>
> The target node decides whether it will accept the atomic action request 38. (Mathias, Col. 3, lines 54-55.)

Mathis does not, therefore, teach or reasonably suggest limitation 1(c).

As to limitation 1(e), the text cited by the office action makes it clear that the determination not to establish a link between the initiating node and the target node is made by the target node, not the discovery machine. Mathis does not, therefore, teach or reasonably suggest limitation 1(e).

Because the combination of Mathis and Hansmann fails to teach or reasonably suggest all of the limitations of claim 1 (as amended), claim 1 (as amended) is patentable over that combination. Additionally, because claims 2-4, 6-8 and 13 depend from claim 1 (as amended), claims 2-4, 6-8 and 13 are patentable over the cited combination.

5. Claim 12 has been rejected under 35 U.S.C. § 103(c) as being obvious over Mathis in view of Hansmann in further view of Waldo.

Claim 12, which depends from claim 1 (as amended), recites the limitation, "wherein determining that said first user will accept said communication further comprises the step of storing notification of said communication if said first user is unavailable." The office asserts that this limitation may be found in Waldo.

Applicant submits that there is no motivation to combine Waldo with Mathis and Hansmann. Mathis is cited as teaching the determining that a user will accept a communication. As noted above, Mathis teaches that this determination is made by the target node. The office action asserts that it "one would have obvious to one of ordinary skill in the art at the time the invention was made for the step of determining that the first user will accept the communication to further comprise the step of storing the notification of the communication if the first user is unavailable. One would be motivated to do so for clients to avoid attempting to access a service that is no longer available (Waldo, Abstract)." (Office Action, p. 12.)

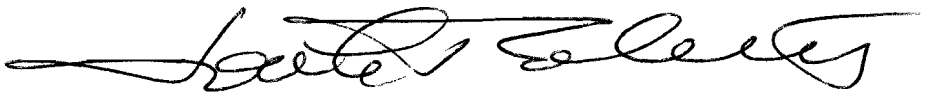
Applicant respectfully submits that the suggested motivation fails to identify a structure that would perform this step. Mathis does not teach a discovery machine. Thus, the only candidate for performing the suggested step is the initiating node. However, in order to store information regarding a failed communication at the initiating node, the initiating node would have to support additional structures capable of knowing the state of the target nodes in the network and capable of updating this state information as the state of the target nodes change. Such a modification of Mathis would impermissibly change the theory of operation of Mathis. Based on the foregoing, Applicant submits that there is no motivation to combine Mathis and Hansmann with Waldo.

Additionally, Applicant has previously demonstrated that the combination of Mathis and Hansmann fails to teach the limitations of claim 1 (as amended). Because claim 12 depends from claim 1 (as amended), claim 12 recites the limitations of that base claim. Waldo is not cited by the office action as curing the deficiencies of the combination of Mathis and Hansmann. For these reasons, claim 12 is patentable over the combination of Mathis, Hansmann and Waldo.

C. CONCLUSIONS

Applicant respectfully submits that this Amendment places the claims in condition for final allowance. Applicant requests that this Amendment be entered and that the current rejection of the claims now pending in this application be withdrawn in view of the above amendments, remarks and arguments. Applicant respectfully requests that if any of the pending claims are not allowed, the examiner contact Applicant's counsel at the number listed below prior to the issuance of another office action in this matter.

Respectfully Submitted,



Jon L. Roberts, Ph.D., J.D.,
Reg. No. 31293
Elliott D. Light, Esq.
Registration No. 51,948
ROBERTS MARDULA & WERTHIEM, LLC
11800 Sunrise Valley Dr.
Suite 1000
Reston, VA 20191
(703) 391-2900